

Seminar 5

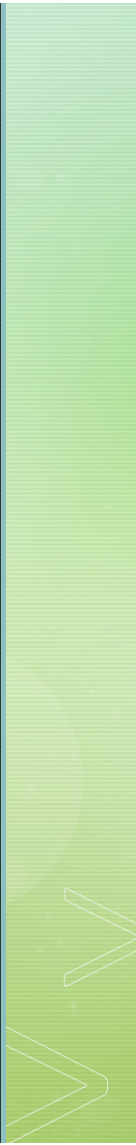
Quantum Search Algorithms

Before Going in...

- Shor's Algorithm was devised in 1994.
- The Quantum Search Algorithm, or Grover's Algorithm, was devised in 1996.
- Yeah..pretty contemporary stuff! You know what this means then!



Before Going in...

- What is Quantum Search Algorithm anyway?
 - Suppose you are given a map containing many cities, and wish to determine the shortest route passing through all cities on the map.
 - Brute Force: Just Draw it all!
- 

Before Going in...

- When the whole graph has N routes, it is obvious that the whole algorithm will require $O(N)$ operations.
- For Quantum Computers, surprisingly, this is viable in $O(\sqrt{N})$ operations!
- Can we do better than $O(\sqrt{N})$?

The Oracle

- Suppose we wish to search through N elements.
- Make indices of those form 1 to N : when $N = 2^n$, n bits will suffice.
- Assume the search algorithm has M solutions:
- Define a function f : If x is a solution for the search algorithm, $f(x)=1$. Else, $f(x)=0$.

The Oracle

- Quantum Oracle: A Black Box with the ability to recognise solutions to the search problem.
- How the oracle functions is a later topic.
- How does the oracle 'recognise'? : Oracle Qubit $|q\rangle$

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle,$$

Hadamard Transform

- Quiz. Apply the oracle transformation at $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.
- Ans. $|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Note that the oracle qubit DOES NOT change during the process.
- Simplification: $|x\rangle \rightarrow (-1)^{f(x)} |x\rangle$
- The oracle *marks* the solutions to the search problem.

Does the Oracle already know the solution?

- *Knowing* and *Recognising* solutions are different subjects.
- Example. Factorisation of m
- Set the oracle to divide m by x if the state $|x\rangle$ comes as the input. If possible, flip the qubit.
- f : 1 if x divides m , 0 if not.
- Then, construct a circuit that makes $|q\rangle \rightarrow |q \oplus f(x)\rangle$
- We know that we construct the relevant quantum circuits.

Prerequisite Procedures

- First, apply the Hadamard Transform to make the equal superposition state $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.
- From here, the search algorithm is consisted of a routine operation called as the *Grover Iteration*.

Grover Iteration

- Grover Iteration consists of Four steps.
- 1. Apply the Oracle O .
- 2. Apply the Hadamard Transform.
- 3. Apply a conditional phase shift: if $|0\rangle$, the state remains the same. For non-zero x , $|x\rangle$ is transformed to $-|x\rangle$.
- 4. Apply the Hadamard Transform again.

Schematic Diagram

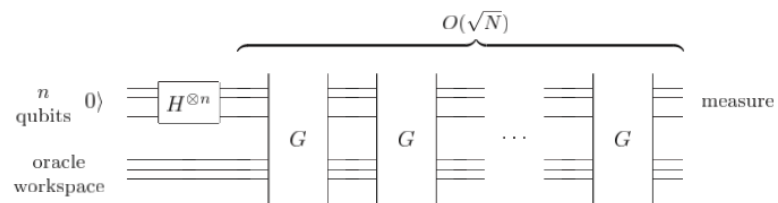


Figure 6.1. Schematic circuit for the quantum search algorithm. The oracle may employ work qubits for its implementation, but the analysis of the quantum search algorithm involves only the n qubit register.

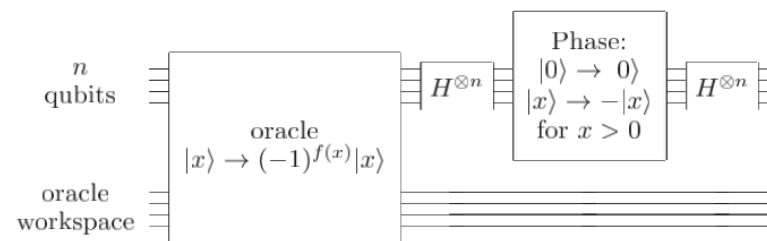


Figure 6.2. Circuit for the Grover iteration, G .

Further Explanations

- Hadamard Transforms can be done with $O(\log n)$ gates.
- Conditional Transforms can be done with $O(n)$ gates.
- The gates required for the oracle will differ by the search required.
- The whole process can be written as $H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}O = (2|\psi\rangle\langle\psi| - I)O$. ($|\psi\rangle$ is the equal superposition state.)
- Quiz.

Exercise 6.2: Show that the operation $(2|\psi\rangle\langle\psi| - I)$ applied to a general state $\sum_k \alpha_k |k\rangle$ produces

$$\sum_k [-\alpha_k + 2\langle\alpha\rangle] |k\rangle,$$

Geometric Visualisation

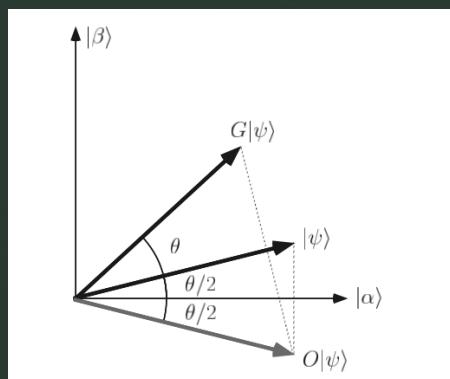
- Question: What does the Grover Iteration do?
- Define $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum'' |x\rangle$, $|\beta\rangle = \frac{1}{\sqrt{M}} \sum' |x\rangle$, meaning that the first ket is an equal superposition of states that are NOT solutions, and the second ket is a superposition of states that ARE solutions.
- $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$: The initial state is spanned by $|\alpha\rangle$ and $|\beta\rangle$.

Geometric Visualisation

- Oracle's Role: Reflection by the $|\alpha\rangle$ -axis
- $2|\psi\rangle\langle\psi| - I$'s Role: Reflection by $|\psi\rangle$
- Set $\cos \frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$: $G|\psi\rangle = \cos \frac{3\theta}{2} |\alpha\rangle + \sin \frac{3\theta}{2} |\beta\rangle$.
- Obviously, $G^k |\psi\rangle = \cos \frac{(2k+1)\theta}{2} |\alpha\rangle + \sin \frac{(2k+1)\theta}{2} |\beta\rangle$.

Summary

- Grover Iteration is an operation that ROTATES the state ket by θ on a 2D space spanned by $|\alpha\rangle$ and $|\beta\rangle$.
- If applied repeatedly, the state ket will eventually be close to $|\beta\rangle$.



Performance

- How many iterations shall we need?
- $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$: we must rotate $\arccos \sqrt{\frac{M}{N}}$ radians to reach $|\beta\rangle$.
- $CI(x)$: integer closest to x
- $R = CI\left(\frac{\arccos \sqrt{\frac{M}{N}}}{\theta}\right)$ iterations rotates $|\psi\rangle$ to within an angle $\theta/2 \leq \pi/4$ of $|\beta\rangle$.

Performance

- If $M \ll N$: $\theta \approx \sin \theta \approx 2 \sqrt{\frac{M}{N}}$: The angular error is at most $\frac{\theta}{2} = \sqrt{\frac{M}{N}}$.
- General Case: $R = CI\left(\frac{\arccos \sqrt{\frac{M}{N}}}{\theta}\right)$ -> Lower limit of theta means upper limit of R
- $\frac{\theta}{2} \geq \sin \frac{\theta}{2} = \sqrt{\frac{M}{N}}$: $R \leq \left\lceil \frac{\pi}{4} \sqrt{\frac{M}{N}} \right\rceil$: Total number of operations is $O\left(\sqrt{\frac{M}{N}}\right)$.

Summary

Algorithm: Quantum search

Inputs: (1) a black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where $f(x) = 0$ for all $0 \leq x < 2^n$ except x_0 , for which $f(x_0) = 1$; (2) $n + 1$ qubits in the state $|0\rangle$.

Outputs: x_0 .

Runtime: $O(\sqrt{2^n})$ operations. Succeeds with probability $O(1)$.

Procedure:

1. $|0\rangle^{\otimes n}|0\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ apply $H^{\otimes n}$ to the first n qubits,
and HX to the last qubit
3. $\rightarrow \left[(2|\psi\rangle\langle\psi| - IO) \right]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$ apply the Grover iteration $R \approx$
 $\lceil \pi\sqrt{2^n}/4 \rceil$ times.
 $\approx |x_0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$
4. $\rightarrow x_0$ measure the first n qubits

Caveats

- Okay... what if M is larger or equal to $N/2$? Then we don't have direct evidence that G will rotate the state close enough to $|\beta\rangle$.
- If it is known that $M > N/2$: Just pick any element and test it. The success rate is more than $1/2$.
- If it is unknown: double the number of elements in the search space by adding N extra items to the search space, none of which are solutions. (i.e. add another qubit to the search index.)

'Deriving' the Quantum Search Algorithm

- Okay..we did this, but how the f*** can we think of it?
- For the sake of simplicity, let's assume there is just one solution to the search algorithm problem: $|x\rangle$
- Step 1. Think of a Hamiltonian that depends on $|\psi\rangle$ and $|x\rangle$, and after some prescribed time, $|\psi\rangle$ evolves to $|x\rangle$.
- Step 2. Simulate this whole action using the Quantum Simulation Algorithm.

The Hamiltonian

- Simple viable solutions: $H = |x\rangle\langle x| + |\psi\rangle\langle\psi|$ or $H = |x\rangle\langle\psi| + |\psi\rangle\langle x|$.
(Actually, both turn out to be solutions!)
- Time evolution: $e^{-iHt}|\psi\rangle \approx (1 - iHt)|\psi\rangle = (1 - it)|\psi\rangle - it\langle x|\psi\rangle|x\rangle$
- OMG! The $|\psi\rangle$ vector is now slightly rotated closer to $|x\rangle$ axis!
Can we make this closer?

The Hamiltonian

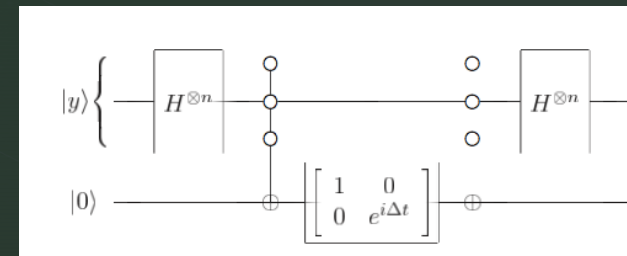
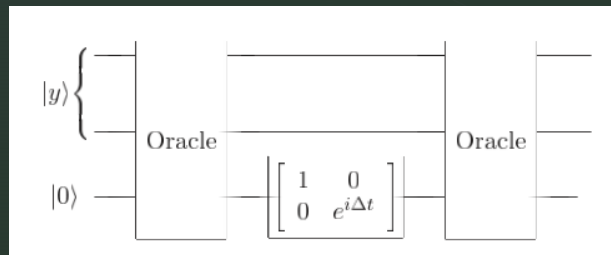
- Orthogonal Bases $|x\rangle$ and $|y\rangle$
- $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$
- Then, $H = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} \alpha^2 & \alpha\beta \\ \beta\alpha & \beta^2 \end{bmatrix} = \begin{bmatrix} 1 + \alpha^2 & \alpha\beta \\ \beta\alpha & 1 - \alpha^2 \end{bmatrix} = I + \alpha(\beta X + \alpha Z)$
- $e^{-iHt}|\psi\rangle = e^{-it}(\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)(\beta X + \alpha Z)|\psi\rangle)$
- Note $(\beta X + \alpha Z)|\psi\rangle = |x\rangle$
- $e^{-iHt}|\psi\rangle = e^{-it}(\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle)$

Analysis

- $e^{-iHt}|\psi\rangle = e^{-it}(\cos(\alpha t)|\psi\rangle - i\sin(\alpha t)|x\rangle)$: When $t = \frac{\pi}{2\alpha}$, we can get $|x\rangle$ with probability 1!
- Problem: α depends on $|x\rangle$.
- Solution: make $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle \rightarrow$ by this way, α is the same regardless of the state ket.

Realisations as Quantum Circuits

- We know the algorithm – let's make it into a Quantum Circuit!
- How do we simulate the Hamiltonians $|x\rangle\langle x|$ and $|\psi\rangle\langle\psi|$?
(To be specific, $e^{-i(|x\rangle\langle x|\Delta t)}$ and $e^{-i(|\psi\rangle\langle\psi|\Delta t)}$)



Links with the Search Algorithm

- What if $\Delta t = \pi$?
- Compare the result with the Grover Iteration:
- Caveat. Brute-Application gives usually gives $O(N)$ (No better than the classical search algorithm.). Actually, $\Delta t = \pi$ is a special case and gives $O(\sqrt{N})$ oracles to be used!

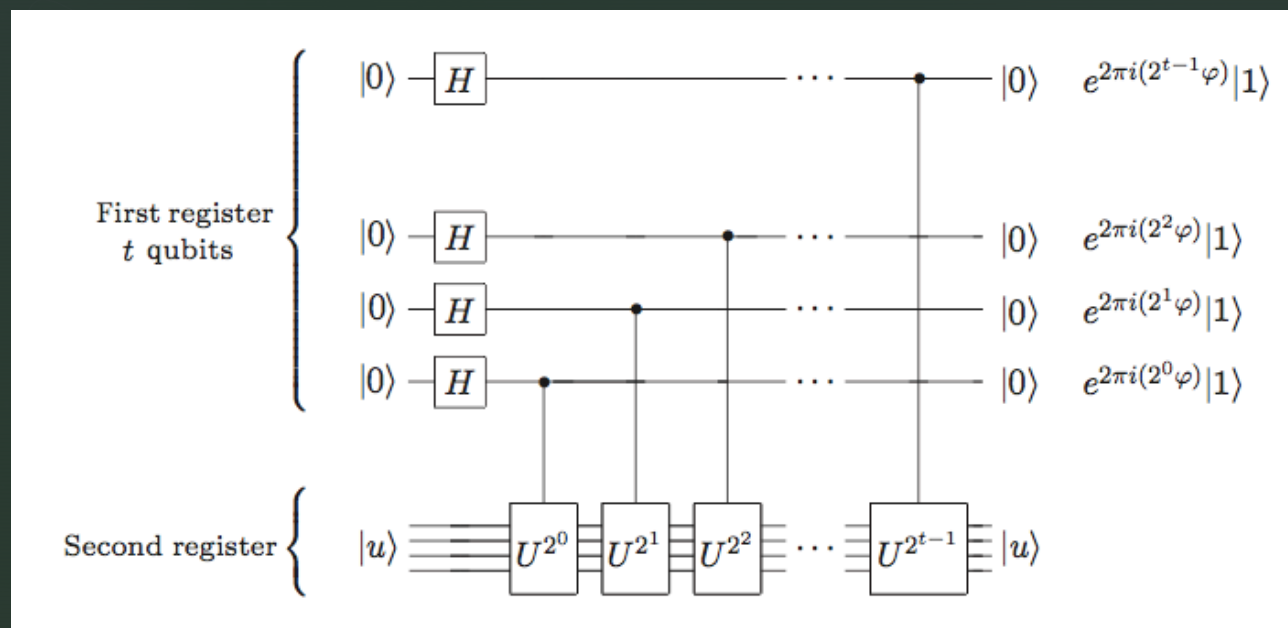
Quantum Counting

- How do we determine the number of solutions in a Quantum Search problem?
- Classical: $O(N)$ (Obviously.)
- How do we do it in Quantum?
- Spoiler Alert: We use Phase Estimation.

The Basics

- Suppose $|a\rangle$ and $|b\rangle$ are the two eigenvectors of the Grover iteration in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$.
- Let θ be the angle of rotation determined by the Grover iteration.
- Little calculation shows that the eigenvalues are $e^{i\theta}, e^{i(2\pi-\theta)}$.
- GOAL: Assume augmented oracle: $\sin^2 \frac{\theta}{2} = \frac{M}{2N}$. Then, estimating theta in a reasonable amount of accuracy shall suffice.

Recall



Approximate Quantum Counting Algorithm

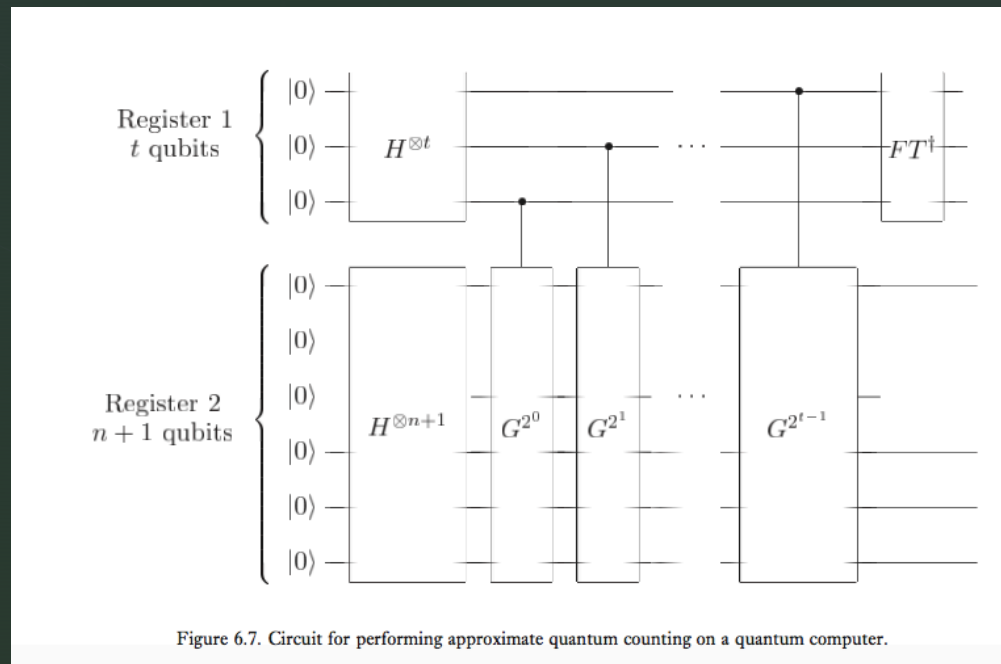


Figure 6.7. Circuit for performing approximate quantum counting on a quantum computer.

Note. $t = m + \log(2 + \frac{1}{2\epsilon})$

Estimation of Error

- Our discussion of this topic last seminar reveals that this circuit can estimate θ or $2\pi - \theta$ with an error of 2^{-m} with an accuracy of $1 - \epsilon$.
- How much does this give on error of M?
- $\frac{|\Delta M|}{2N} = \left| \sin^2 \frac{\theta + \Delta\theta}{2} - \sin^2 \frac{\theta}{2} \right|$
- Simple calculation gives $\frac{|\Delta M|}{2N} < \left(2\sin \frac{\theta}{2} + \frac{|\Delta\theta|}{2} \right) \frac{|\Delta\theta|}{2}$ or
- $|\Delta M| < \left(\sqrt{2MN} + \frac{N}{2^{m+1}} \right) 2^{-m}$

Speeding up NP-complete problems

- Example. Hamiltonian Cycles (HC): A simple cycle which visits every vertex of the graph.
- How to solve: 1. Label the vertices. (Repetition ALLOWED)
- 2. Check each ordering to see whether it is the solution. (Simple and clear, isn't it?)
- Total: $n^n = 2^{n \log n}$ processes.
- Solving NP problems are similar to this: if a problem of size n has witnesses which can be specified using $w(n)$ (Polynomial) bits, then searching through all $2^{w(n)}$ possible witnesses will suffice.

The Quantum-Way

- I won't go in details. Just think that we construct the oracle accordingly, and perform the search algorithm.
- Normally, the quantum way requires $p(n)2^{n \log n / 2}$ operations. This is roughly the square root of the classical algorithm if viewed asymptotically.
- $P(n)$ emerges because constructing oracle requires operations.

Search in an Unstructured Database

- How do we find Chrysanthemum in a database that contains 10,000 flowers?
- Suppose we have a database containing $N \equiv 2^n$ items, each of length l bits. We will label these items d_1, d_2, \dots, d_N .
- CPU: Stores small amount of information, data manipulation takes place.
- Memory: Stores the database, PASSIVE storage.

Classical Algorithm

- Rather brute force...
- Set an n-bit index. The CPU must be able to store this information.
- We compare it one-by-one: 1. The database entry corresponding to the index is loaded.
- 2. Compare to the string we want to search.
- 3. Match -> Output the value and Halt. No Match -> value increases.

The 'Quantum' CPU

- CPU is consisted of 4 registers;
- (1) an n qubit 'index' register initialized to $|0\rangle$;
- (2) an l qubit register initialized to $|s\rangle$ and remaining in that state for the entire computation;
- (3) an l qubit 'data' register initialized to $|0\rangle$;
- and (4) a 1 qubit register initialized to $(|0\rangle - |1\rangle)/\sqrt{2}$.

'Quantum' Memory

- Two ways of Implementation:
 1. Quantum memory containing all the information, and $|d_x\rangle$ as the entries.
 2. Use classical memory. However, it can be addressed by an index x which can be in a superposition of MULTIPLE values.
- Therefore, a superposition of values can be loaded!

The Oracle

- Loading: the CPU's index register is in the state $|x\rangle$ and the data register is in the state $|d\rangle$.
- then the contents d_x of the x th memory cell are added to the data register: $|d\rangle \rightarrow |d \oplus d_x\rangle$.
- What the oracle must do: flip the phase when it is the answer!
- Assume starting at $|x\rangle|s\rangle|0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

The Oracle

- Then, the CPU loads the data: $|x\rangle|s\rangle|d_x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- The Second and Third registers are compared. If same, return $-|x\rangle|s\rangle|d_x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and if different, $|x\rangle|s\rangle|d_x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
- Finally, load the data again. This will make the state to be $|x\rangle|s\rangle|0\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ once again.

Some Analysis

- By our results in Quantum Search Algorithms, we require $O(\sqrt{N})$ operations of loading, instead of $O(N)$ in classical.
- Can the memory be implemented classically?
Answer: Yes, but with some limitations. This is referred as the Quantum Addressing Scheme. See P.268 in Nielsen and Chuang for conceptual details.

Practicality

- 1. There is no such thing as 'unstructured' database. It can be complex and be similar to being unstructured, but it is little different.
- 2. The Quantum Addressing Scheme ruins the practicality. The scheme requires $O(N \log N)$ operations, which is not the best optimisation one will hope for.

Optimality of the Search Algorithm

- We have shown that in a database that has N entries, with the Quantum Search Algorithm, we can do it in $O(\sqrt{N})$ operations.
- Is this the best you can do?
- Answer: Yes. No quantum algorithm can perform this task using fewer than $\Omega(\sqrt{N})$ accesses to the search oracle, and thus the algorithm we have demonstrated is optimal.
- Let's prove it!

Assumptions

- The algorithm starts with $|\psi\rangle$, and assume that the search problem has only one solution $|x\rangle$.
- We have access to a general oracle, which returns a phase shift of -1 if the state is a solution, and 1 if not. In other words, $O_x = I - 2|x\rangle\langle x|$.
- Define $|\psi_k^x\rangle = U_k O_x U_{k-1} O_x \dots U_1 O_x |\psi\rangle$: The oracle is accessed k times, and obviously, the gap is filled by unitary operations.
- Define $|\psi_k\rangle = U_k U_{k-1} \dots U_1 |\psi\rangle$: This time, all the unitary operations are done, but the oracle is never accessed.

Our Strategy

- Define Deviation $D_k = \sum_x \|\psi_k^x - \psi_k\|^2$. I omitted the bra-ket symbol. If this quantity is small, we cannot 'extract' the solutions with high probability.
- We will use two steps to prove our assumption.
- Step 1. There exists a bound of D_k that it cannot grow faster than the rate of $O(k^2)$.
- Step 2. D_k must be $O(N)$ to distinguish N alternatives with at least a probability of $\frac{1}{2}$.

Induction

- Assume that $D_k \leq 4k^2$ for k . Obviously, this is true for $k=0$.
- Then, $D_{k+1} = \sum_x \|O_x \psi_k^x - \psi_k\|^2$. Note that U_{k+1} is unitary, and therefore squaring it will return 1.
- $D_{k+1} = \sum_x \|O_x \psi_k^x - \psi_k\|^2 = \sum_x \|O_x(\psi_k^x - \psi_k) + (O_x - I)\psi_k\|^2$, and apply $\|b + c\|^2 \leq \|b\|^2 + 2\|b\|\|c\| + \|c\|^2$.

Induction

- This returns $D_{k+1} \leq \sum_x \|\psi_k^x - \psi_k\|^2 + 4\|\psi_k^x - \psi_k\| |\langle x|\psi_k \rangle| + 4|\langle x|\psi_k \rangle|^2 \leq D_k + 4\sqrt{D_k} + 4$. Note $\sum_x |\langle x|\psi_k \rangle|^2 = 1$ and the second term is calculated using Cauchy-Schwarz Ineq.
- Putting $D_k \leq 4k^2$ returns $D_{k+1} \leq 4k^2 + 8k + 4 = 4(k+1)^2$.
- The induction is completed.

Distinguishing Solutions

- Assume that $|\langle x | \psi_k^x \rangle|^2 \geq 1/2$.
- Define $E_k = \sum_x \|\psi_k^x - x\|^2$. In this case, $E_k = \sum_x \|\psi_k^x - x\|^2 \leq \sum_x 2 - 2\langle x | \psi_k^x \rangle \leq (2 - \sqrt{2})N$.
- Define $F_k = \sum_x \|x - \psi_k\|^2$.
- $D_k = \sum_x \|(\psi_k^x - x) + (x - \psi_k)\|^2 \geq \sum_x \|\psi_k^x - x\|^2 - 2 \sum_x \|\psi_k^x - x\| \|x - \psi_k\| + \sum_x \|x - \psi_k\|^2 = E_k + F_k - 2 \sum_x \|\psi_k^x - x\| \|x - \psi_k\|$

Distinguishing Solutions

- Apply Cauchy-Schwarz for the last term: $\sum_x \|\psi_k^x - x\| \|x - \psi_k\| \leq \sqrt{E_k F_k}$
- Combining the results gives $D_k \geq E_k + F_k - 2 \sum_x \|\psi_k^x - x\| \|x - \psi_k\| \geq E_k + F_k - 2\sqrt{E_k F_k} = (\sqrt{F_k} - \sqrt{E_k})^2$
- Simple calculation gives $F_k \geq 2N - 2\sqrt{N}$. Combining this with minimum of E_k gives $D_k \geq 0.42N$ for sufficiently large N .
- The proof has been concluded.

Solutions for the Search Problem

- The search algorithm can be summarised as finding solutions to a function f : If x is a solution for the search algorithm, $f(x)=1$. Else, $f(x)=0$.
- FUNDAMENTAL PROBLEM: Does this solution exist? How can we be sure?
- Actually, this problem is equally difficult as the search problem itself.
- Let's define the function for this problem as F . F , in general, is definitely a boolean function.

Defining Functions

- Let $D(F)$ to be the minimum number of oracle access for a Classical computer to perform to determine F by certainty.
- $Q_2(F)$: Minimum number of oracle access for a Quantum computer requires to determine F by probability $2/3$. $2/3$ is actually arbitrary – more than $1/2$ is sufficient.
- $Q_0(F)$: Minimum number of oracle access for a Quantum computer requires to determine F by either certainly or inconclusively.
- $Q_E(F)$: Minimum number of oracle access for a Quantum computer requires to determine F by certainty.
- Obviously, $N \geq D(F) \geq Q_E(F) \geq Q_0(F) \geq Q_2(F)$

Method of Polynomials

- We now construct a minimum degree polynomial to *represent* a Boolean function $F(X)$.
- *Represent?:* For all $X \in \{0,1\}^N$, $p(X) = F(X)$, p is the polynomial.
- Suitable candidate: $p(X) = \sum_{Y \in \{0,1\}^N} F(Y) \prod_{k=0}^{N-1} [1 - (Y_k - X_k)^2]$
- Important property: The minimum degree polynomial representing $F(X)$ is unique.
- It has been proven that $D(F) \leq 2 \deg(F)^4$

More Properties and Functions

- 'Approximating' Polynomial: A polynomial such that for all x , $|p(X) - F(X)| \leq 1/3$. $\widetilde{\deg}(F)$ denotes the degree.
- Properties: $\widetilde{\deg}(\text{OR}), \widetilde{\deg}(\text{AND}) \in \Theta(\sqrt{N})$
 $D(F) \leq 216 \widetilde{\deg}(F)^6$
- Quiz. Show that $P(X) = 1 - (1 - X_0)(1 - X_1) \dots (1 - X_{N-1})$ represents OR.

Linking with Quantum Circuits

- Let's think of a quantum algorithm Q which performs T queries to the oracle.
- We can represent $Q = \sum_{k=0}^{2^n-1} c_k |k\rangle$
- Theorem. c_k are polynomials of degrees at most T . The proof is accessible, but I won't delve deep in this.

Results

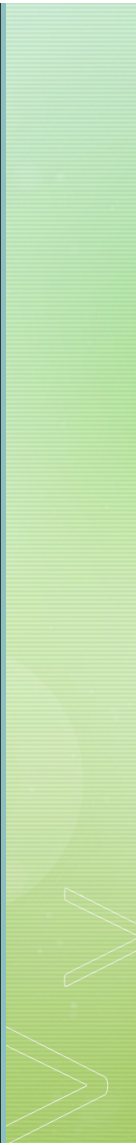
- As c_k has a minimum degree of T , probability will obviously have a degree of $2T$.
- Case 1. $P(X)=F(X)$ with certainty. $\deg(F) \leq 2T$. Therefore,
$$Q_E(F) \geq \frac{\deg(F)}{2}.$$
- Case 2. Approximation. Analogously, $Q_2(F) \geq \frac{\widetilde{\deg(F)}}{2}.$

Results and Caveats

- Compare $D(F) \leq 2 \deg(F)^4$, $D(F) \leq 216 \widetilde{\deg}(F)^6$ with $Q_E(F) \geq \frac{\deg(F)}{2}$, $Q_2(F) \geq \frac{\widetilde{\deg}(F)}{2}$.
- $Q_E(F) \geq \left[\frac{D(F)}{32} \right]^{1/4}$ and $Q_2(F) \geq \left[\frac{D(F)}{13824} \right]^{1/6}$.
- Black box method only provides polynomial speedups compared to classical algorithms AT MOST.
- Even this is in many cases impossible.
- However, it is known that for $F=\text{OR}$ and $D(F)=N$, $Q_2(F) \in \Omega(\sqrt{N})$.
What is this algorithm?



Before Finishing...

- The Fourier Transform and the Search Algorithm provides both the revolutionary aspects of Quantum computing as well as its limitations.
 - Until now, our work was mostly theoretical; first we looked at Quantum circuits and expanded it to applications.
 - The next seminar will be different – we will discuss the real world implementations of Quantum Computing.
- 

Before Finishing...

- Also, it is easily conceivable that non-ideal real world implementations will have some differences from the idealistic circuits we have seen.
- Is information lost? Are there noises? How can we measure and reduce it?
- These are the basic concepts of Quantum Information Theory, which will be the second part of Nielsen and Chuang.